Scalar Product Lattice Computation for Efficient Privacy-preserving Systems

Yogachandran Rahulamathavan, Safak Dogan, *Senior Member, IEEE*, Xiyu Shi, *Member, IEEE*, Rongxing Lu, *Senior Member, IEEE*, Muttukrishnan Rajarajan, *Senior Member, IEEE*, and Ahmet Kondoz, *Senior Member, IEEE*

Abstract—Privacy-preserving applications allow users to perform on-line daily actions without leaking sensitive information. The privacy-preserving scalar product is one of the critical algorithms in many private applications. The state-of-the-art privacy-preserving scalar product schemes use either computationally intensive homomorphic (public-key) encryption techniques such as Paillier encryption to achieve strong security (i.e., $128-$bit) or random masking technique to achieve high efficiency for low security. In this paper, lattice structures have been exploited to develop an efficient privacy-preserving system. The proposed scheme is not only efficient in computation as compared to the state-of-the-art but also provides high degree of security against quantum attacks. Rigorous security and privacy analyses of the proposed scheme have been provided along with a concrete set of parameters to achieve $128-$bit and $256-bit$ security. Performance analysis shows that the scheme is at least five orders faster than the Paillier schemes and at least twice as faster than the existing randomisation technique at $128-$bit security. Also the proposed scheme requires six-time fewer data compared to Paillier and randomisation based schemes for communications.

Index Terms—Lattice-based cryptography, privacy-preserving techniques, scalar product computation.

1 Introduction

Regulators around the world are enforcing privacy-by-design and privacy-by-default approaches to protect the users' data in rest, transit and processing. Several service providers and applications that traditionally use users' data in plain domain to extract patterns and provide services are now applying encrypted domain computations. Some of the example applications are disease classification in healthcare, data search in the cloud, biometric verification, etc. (e.g., [1]–[8] and references their-in). The common theme across these applications is that there are two distrusting parties want to work on a common goal by combining both of their data while preserving the data privacy. For example, a buyer wants to verify his age to an on-line shop using security token instead of sending date of birth.

There are algorithms developed in literature to support data privacy for applications such as classification algorithms, data mining algorithms, distance calculations etc. [1]–[8]. In all of these algorithms, one party encrypts the sensitive data whenever that data should be sent to other party. Hence the second party needs to process the received data in an encrypted domain. This approach ensures data privacy. Regardless of algorithms, privacy-preserving scalar product (PPSP) has been used as one of the privacy enabling tools between the two parties. The intuition behind this is that a mathematical function that relies on two different variables can be modified into a scalar product [3], [4]. Therefore, PPSP becomes a vital tool in most of the privacy-preserving (PP) algorithms.

Suppose, there are two parties, A and B, want to compute the following scalar product

$$\mathbf{a}^T\mathbf{b} = \sum_{i=1}^{n} a_i.b_i,$$

where vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ belongs to A and vector $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ belongs to B. The privacy requirement here is that no party is allowed to learn the others input vector. At the end, only one party can learn the output of the scalar product (SP).

Several solutions have been proposed to address this problem in literature (see Section 2). These solutions rely on either public-key encryption techniques to achieve strong security or randomisation techniques for high efficiency. The security of these schemes rely on mathematically hard problems and these solutions will be obsolete in few years time due to the rise of quantum computers as there are existing quantum algorithms which can easily solve the mathematically intractable problems [9]–[13].

Hence, this paper exploits *lattice-based cryptography* to build a PPSP. The proposed model is similar to lattice-based fully homomorphic encryption scheme [9] and support multiple encryption and addition without decryption [11]. However, the major challenge was to ensure the error terms are not overflowed to effect the accuracy. The paper proposes a methodology to control the error terms while

- *Y. Rahulamathavan, S. Dogan, X. Shi and A. Kondoz are with the Institute for Digital Technologies, Loughborough University London, London, U.K. (e-mails: {y.rahulamathavan, s.dogan, x.shi, a.kondoz}@lboro.ac.uk).*
- *R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada. (e-mail: RLU1@unb.ca).*
- *M. Rajarajan is with the Information Security Group, School of Engineering and Mathematical Sciences, City University London, EC1V 0HB, London, U.K. (e-mails: R.Muttukrishnan@city.ac.uk).*
- *The work was supported by UK-India Education Research Initiative (UKIERI) through grant UGC-UKIERI-2016-17-019.*
- *Source code for this work can be found in Github repo (https://github.com/rahulay1/LWE)*

ensuring the given security level, i.e., 128-bit.

Lattice-based cryptography has been proven to be secure against quantum attacks and expected to replace the existing public-key cryptography schemes [9]–[13]. Therefore the proposed solution will be secure against quantum computers and can be used in PP algorithms for various applications to achieve privacy. At the same time, the experimental results (see Section 6) show that the proposed PPSP can also be executed significantly faster than the existing PPSP schemes at equivalent security level.

The rest of this paper is organised as follows: The related work is discussed in Section 2. The background information about lattice-based cryptography and its hardness assumptions are provided in Section 3. The proposed algorithm is described in Section 4 followed by the security analysis and parameter selections in Section 5. Experimental results are provided in Section 6. The conclusions and future work are discussed in Section 7.

2 Literature Review

The existing PPSP schemes can broadly be divided into two: 1) the schemes that are built using proven cryptography such as homomorphic encryption, and 2) the schemes that are built based on information theory such as randomisation and linear algebra. Even though the latter is much efficient than former, security level of latter is not quantified. The following subsections study the state-of-the-art algorithms for each of these schemes.

2.1 Homomorphic encryption based PPSP

Homomorphic encryption techniques such as Paillier play a vital role in supporting PPSP since it offers high security such as $128-$bits [21]. Even though this scheme is highly secure, it becomes inefficient with the size of the vectors i.e., it may take long time (i.e., a few minutes in modern laptops with five cores and 6GB memory) to compute the scalar product when the dimension of the vectors is around 1000. Several efficient PPSP schemes were proposed in literature to improve the efficiency [20], [22], [24]–[30]. All these schemes use the homomorphic PPSP scheme as a benchmark to measure the efficiency. We discuss these in the following subsections.

A lattice based functional encryption technique that *predicates* whether the SP is equivalent to 0 or not 0 was proposed in [18]. This work is based on lattice trapdoors [16]. If the SP is equivalent to 0 then the trapdoors successfully remove large elements in the problem. Note that the work in [18] is completely different to the objective of the proposed work on this paper and the algorithm in [18] cannot be modified to develop a PPSP scheme.

There are works that directly uses Learning with errors based cryptographic scheme for encrypted domain matrix calculations [34]–[37]. These works treat the encryption technique as a black-box to develop several applications ranging from logistic regression based prediction to statistics of smart meter reading in encrypted domain. In contrast to traditional homomorphic encryption such as Paillier, the learning with error based encryption involve a number of parameters that must be set properly for problems with different dimensions. Otherwise, as we will show in Section 3, error terms will overflow and decryption will be unsuccessful. In this paper, we clearly show how to setup the parameters to achieve different level of security. **Most importantly this is the first paper that compares the performance of quantum secure cryptographic scheme against traditional homomorphic encryption scheme and information theoretic secure scheme and show that a quantum cryptographic based scheme can outperform the other schemes if the parameters are set properly.**

2.2 Information theory based PPSP

In 2001, Du et al proposed a PPSP algorithm using 1-out-of-N oblivious transfer function and homomorphic encryption [24]. This algorithm is based on splitting the input vector $\mathbf{a}$ of Party A into p number of random vectors to achieve privacy from Party B. The drawback of this method is that both parties need to be on-line and interact several times to perform the SP.

In 2002, Du et al proposed another SP which reduces the communication complexity of their previous work [24] but with the help of a third-party semi-trusted server [25]. The algorithm in [25] requires a third-party sever to generate two random vectors $\mathbf{R}_A$ and $\mathbf{R}_B$. The vector $\mathbf{R}_A$ will be revealed to A and the vector $\mathbf{R}_B$ will be revealed to B. Using these vectors, A and B compute the shares of the SP. Hence, both the parties must reveal their shares to get the actual SP value. The communication complexity of this protocol is four times higher than the communication cost of SP without privacy. Moreover, the major draw back of this work is the involvement of third-party who can easily collude with one of the parties to reveal the other party's input vector.

Vaidya and Clifton in 2002 proposed a novel PPSP solution but without the need of third-party in [26]. The communication complexity of the algorithm in [26] is same as [25]. However, the computation cost is $O(n^2)$ while it is $O(n)$ for the [25]. Moreover, the security of the SP algorithm in [26] depends on the difficulty of solving $n/2$ linear equations.

In 2007, Amirbekyan et. al. proposed a homomorphic encryption and randomisation (or add vector protocol) based PPSP [27]. Since $2\mathbf{a}^T.\mathbf{b} = \sum_{i=1}^{n} a_i^2 + \sum_{i=1}^{n} b_i^2 - (\mathbf{a}-\mathbf{b})^2$, the authors of [27] exploited homomorphic encryption technique to compute $\mathbf{a}-\mathbf{b}$. Party A generates public and private key pairs using any homomorphic encryption scheme that offers additive homomorphism (i.e., Pailler encryption) and encrypt the elements of vector $\mathbf{a}$. The encrypted vector and the public key are sent to Party B. Party B subtract its vector $\mathbf{b}$ from encrypted $\mathbf{a}$ using homomorphic properties and obtain encrypted $(\mathbf{a}-\mathbf{b})$. Subsequently, Party B permutes and sends the elements of encrypted $(\mathbf{a}-\mathbf{b})$ to Party A. Party A decrypts the vector received from Party B and obtains the permuted $(\mathbf{a}-\mathbf{b})$. Party A also receives $\sum_{i=1}^{n} b_i^2$ from Party B. Using these, Party A can compute the required SP. Similarly, there are several variations of PPSP algorithms proposed in literature they either use homomorphic encryption or randomisation or both [28]–[30].

One of the algorithms that is secure and lightweight to-date is called Secure and Privacy-preserving Opportunistic

Computing proposed in [20] which is proven to be faster than all the other SP and achieve high security. In [20], the security and privacy of the input vectors are protected by masking them by large random integers whose size is around 512 bits. It is shown in [20], that the computational complexity is almost negligible and communication complexity is almost half compared to the Paillier homomorphic encryption based SP [21]. To make a fair comparison with the proposed scheme, we reset the parameters to achieve $128-$bit security against traditional computers. Then in Section 6, we compare the performance of [20] against the proposed lattice-based PPSP scheme and show that the latter one is, at least twice as fast as the [20] algorithm.

Recently, linear algebra based PPSP was proposed in [22] for biometric identification. The solution proposed is efficient and do not require parties to be on-line. In particular, the solution is very useful when Party A wants to outsource the SP computation to Party B.

For this scheme, Party A holds both the input vectors $\mathbf{a}$ and $\mathbf{b}$. Initially, Party A obtains a diagonal matrix $\mathbf{A}$ using the input vector $\mathbf{a}$ followed by generating two random invertable matrices $\mathbf{M}_1$ and $\mathbf{M}_2$ and a random lower triangular matrix $\mathbf{U}$. The encryption of the input vector $\mathbf{a}$ is simply a matrix multiplication i.e., $\mathbf{M}_1\mathbf{U}\mathbf{A}\mathbf{M}_2$. This encrypted matrix is send to Party B. Later, if Party A wants to compute a SP $\mathbf{a}^T\mathbf{b}$ then Party A generates a random lower triangular matrix $\mathbf{V}$ and computes $\mathbf{M}_1^{-1}\mathbf{V}\mathbf{B}\mathbf{M}_1^{-1}$ as an encryption of $\mathbf{b}$ where matrix $\mathbf{B}$ is just a diagonal matrix of $\mathbf{b}$. This encrypted matrix is sent to Party B who computes the following which is equivalent to $\mathbf{a}^T\mathbf{b}$: $\mathbf{Tr}\{\mathbf{M}_1^{-1}\mathbf{V}\mathbf{B}\mathbf{M}_2^{-1}.\mathbf{M}_1\mathbf{U}\mathbf{A}\mathbf{M}_2\}$ where $\mathbf{Tr}$ is a matrix trace operation [19].

This model has been applied in various biometric authentication applications. For example, recently, the work in [23] exploited this scheme to protect biometric templates. In [23], the user extracts biometric template $\mathbf{a}$ and encrypts using random matrices as explained in the previous paragraph. Later, if the user wants to authenticate to the server, then the user extracts a new biometric sample, lets say $\mathbf{b}$, and encrypts using the random matrices and send it to server. Using these encrypted samples (i.e., $\mathbf{a}$ and $\mathbf{b}$), the server can find the similarities. This model requires multiplication of several matrices and the complexity will increase substantially when the elements of the matrices are set to large integers to achieve $128-$bit or higher security. Again, the security of these schemes are dependent on integer factorisation and vulnerable for quantum algorithms.

3 Lattice based Cryptography

Notations

We use bold lower-case letters like $\mathbf{x}$ to denote column vectors; for row vectors we use the transpose $\mathbf{x}^T$. We use bold upper-case letters like $\mathbf{A}$ to denote matrices, and identify a matrix with its ordered set of column vectors. We denote horizontal concatenation of vectors and/or matrices using vertical bar, e.g., $[\mathbf{A}|\mathbf{A}.\mathbf{x}]$ where . denotes the matrix multiplication. For any integer $q \geq 2$, we use $\mathbb{Z}_q$ to denote the ring of integers modulo q, $\mathbb{Z}_q^{n\times m}$ to denote the set of $n \times m$ matrix with entries in $\mathbb{Z}_q$. We denote a real number x as $x \in \mathbb{R}$.

3.1 Lattices

An $m-$*dimensional lattice* Λ is a full-rank discrete subgroup of $\mathbb{R}^m$ [12]. Let $\mathbf{b}_1,\ \mathbf{b}_2, \ldots, \mathbf{b}_n$ denote the n linearly independent vectors in $\mathbb{R}^m$. Then $m-$*dimensional lattice* Λ is defined to be the set of all integer combinations of $\mathbf{b}_1,\ \mathbf{b}_2, \ldots, \mathbf{b}_n$ as follows:

$$\Lambda = \sum_{i=1}^{n} x_i \mathbf{b}_i, \tag{1}$$

where $x_i \in \mathbb{Z}, \forall i$. The set of vectors $\mathbf{b}_1,\ \mathbf{b}_2, \ldots, \mathbf{b}_n$ is called *basis* for the lattice Λ, and n is called the rank of the lattice.

Without loss of generality, we consider *integer lattices* i.e., whose points have coordinates in $\mathbb{Z}^m$. Among these lattices, many cryptographic applications use a particular family of so-called "$q-$ary" integer lattices which contain $q\mathbb{Z}^m$ as a sub-lattice for some small integer q. There are two different $q-$ary lattices considered in many lattice-based cryptographic applications. Let us define them as follows:

3.1.1 $\Lambda_q^{\perp}(A)$

For instance, for any integer $q \geq 2$ and any $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a set of vectors $\mathbf{e} \in \mathbb{Z}^m$ that satisfy the following equation

$$\mathbf{A}.\mathbf{e} = \mathbf{0}\ mod\ q \tag{2}$$

forms a lattice of dimension m, which is closed under congruence modulo q. This lattice is denoted by $\Lambda_q^{\perp}(A)$ where

$$\Lambda_q^{\perp}(A) := \{\mathbf{e} \in \mathbb{Z}^m | \mathbf{A}.\mathbf{e} = \mathbf{0}\ mod\ q\}. \tag{3}$$

Using $\Lambda_q^{\perp}(A)$, we define a coset or shifted lattice $\Lambda_q^{\mathbf{u}}(A)$ where

$$\begin{aligned} \Lambda_q^{\mathbf{u}}(A) &:= \{\mathbf{e} \in \mathbb{Z}^m | \mathbf{A}.\mathbf{e} = \mathbf{u}\ mod\ q\}, \\ &= \Lambda_q^{\perp}(A) + \mathbf{x}, \end{aligned} \tag{4}$$

where $\mathbf{u} \in \mathbb{Z}_q^n$ is an integer solution to

$$\mathbf{A}.\mathbf{x} = \mathbf{u}\ mod\ q. \tag{5}$$

3.1.2 $\Lambda(A^T)$

Similarly, we can define another $m-$dimensional *q-ary* lattice, $\Lambda(A^T)$. For a set of vectors $\mathbf{e} \in \mathbb{Z}^m$, and $\mathbf{s} \in \mathbb{Z}_q^n$ which satisfy the following equation:

$$\mathbf{e} = \mathbf{A}^T.\mathbf{s}\ mod\ q \tag{6}$$

where

$$\Lambda(A^T) := \{\mathbf{e} \in \mathbb{Z}^m | \mathbf{s} \in \mathbb{Z}_q^n\ s.t.\ \mathbf{e} = \mathbf{A}^T.\mathbf{s}\ mod\ q\}. \tag{7}$$

It is easy to check that $\Lambda_q^{\perp}(A)$ and $\Lambda(A^T)$ are dual lattices.

3.2 Lattice Hard Problems

There are three well-known hard problems in lattice that have been exploited by researchers to build several cryptographic applications. This section defines these hard problems briefly.

3.2.1 Short integer solution

Hardness of finding a short integer solution (SIS) was first exploited by Ajtai [10]. The SIS has served as a foundation for many cryptographic applications such as one-way hash

function, identification scheme and digital signature using lattices. The SIS can be defined as follows:

Definition for SIS

For a given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, forming columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, finding a non-zero *short* integer vector $\mathbf{z} \in \mathbb{Z}^m$ with norm $||\mathbf{z}|| < \beta$ such that

$$\mathbf{Az} = \sum_{i=1}^{m} \mathbf{a}_i.z_i = \mathbf{0}\ mod\ q$$

is intractable.

This problem has the following useful observations:

1) Without the requirement of $||\mathbf{z}|| < \beta$ i.e., "short" solution, it is easy to find a vector $\mathbf{z}$ via Gaussian elimination that satisfies $\mathbf{Az} = \mathbf{0}\ mod\ q$.
2) The problem becomes easier to solve if m is increased and difficult to solve if n is increased.
3) The norm bound β and the number m of the column vectors must be large enough that a solution is guaranteed to exist. This is the case when $\beta > \sqrt{n.log(q)}$.

3.2.2 Inhomogeneous short integer solution

Inhomogeneous short integer solution (ISIS) is a variant of SIS. ISIS problem can be defined as follows [11], [12]:

Definition for ISIS

For a given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, forming columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and a uniform random vector $\mathbf{u} \in \mathbb{Z}_q^n$, finding a non-zero integer vector $\mathbf{z} \in \mathbb{Z}^m$ with norm $||\mathbf{z}|| < \beta$ such that

$$\mathbf{Az} = \sum_{i=1}^{m} \mathbf{a}_i.z_i = \mathbf{u}\ mod\ q$$

is intractable.

3.2.3 Learning with errors

Learning with errors (LWE) [9], [13] is an encryption-enabling lattice-based problem but similar to SIS. To enable encryption, the LWE problem depends on a "small" error distribution over integers. The LWE is parametrised by positive integers n and q, and a small error distribution $\mathcal{X} \in \mathbb{Z}_q$, which is typically be a "rounded" normal distribution with mean 0 and standard deviation $\frac{\alpha q}{2\pi}$. The constant α plays a critical role in the security of LWE and it should be chosen as large as possible while satisfying the following condition [9]:

$$\alpha q > 2\sqrt{n}. \tag{8}$$

There are two versions of LWE based problems. Before defining these, let us define a distribution called *LWE-distribution* as follows:

LWE Distribution

For a given *secret* vector $\mathbf{s} \in \mathbb{Z}_q^n$, a sample from LWE distribution $\mathcal{A}_{\mathbf{s},\mathcal{X}} \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ is obtained by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random, a "small" error $e \in \mathcal{X}$, and outputting $(\mathbf{a}, b = \mathbf{s}^T\mathbf{a} + e\ mod\ q)$.

Using the LWE distribution, we can define two versions of LWE problem as follows:

1. Search-LWE

Given m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ drawn from the above LWE distribution $\mathcal{A}_{\mathbf{s},\mathcal{X}}$ for a uniformly random $\mathbf{s} \in \mathbb{Z}_q^n$ (fixed for all samples), it is intractable to find $\mathbf{s}$.

2. Decision-LWE

Given m independent samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where every sample is distributed according to either: (1) $\mathcal{A}_{\mathbf{s},\mathcal{X}}$ for a uniformly random $\mathbf{s} \in \mathbb{Z}_q^n$ (fixed for all samples), or (2) the uniform distribution, then distinguishing which is the case is intractable.

We can have the following observations from the two LWE problems outlined above:

1) Without the error term $e \in \mathcal{X}$, the search-LWE problem can be solved easily using Gaussian elimination technique and the secret $\mathbf{s}$ can be recovered.
2) Similarly for decision-LWE problem, without the error term $e \in \mathcal{X}$, Gaussian elimination technique will reveal with high probability that no solution $\mathbf{s}$ exists if it is not sampled from LWE distribution.
3) If there are m LWE samples $(\mathbf{a}_i, b_i) \leftarrow \mathcal{A}_{\mathbf{s},\mathcal{X}}$ for a uniformly random $\mathbf{s} \in \mathbb{Z}_q^n$ (fixed for all samples), we can combine all $\mathbf{a}_i$s into a matrix $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m] \in \mathbb{Z}_q^{n \times m}$, b_is into a vector $\mathbf{b} = [b_1, b_2, \ldots, b_m]^T$, and e_is into a vector $\mathbf{e} = [e_1, e_2, \ldots, e_m]^T$ into the following vector-matrix linear equation

$$\mathbf{b}^T = \mathbf{s}^T\mathbf{A} + \mathbf{e}^T\ (mod\ q).$$

In the following sections, we will exploit the above lattice hard problems to develop the the lattice-based PPSP.

4 Lattice-based PP Scalar Product Computation

Let us suppose, there are two distrusting entities, X and Y. Entity X owns an $m-$dimensional binary vector $\mathbf{x} \in \{0,1\}^m$. Entity Y owns another $m-$dimensional binary vector $\mathbf{y} \in \{0,1\}^m$. Both X and Y want to interact with each other to compute the SP $s = \mathbf{x}^T\mathbf{y}$ without revealing their own vector to the other party. In the end, one-party obtains $s = \mathbf{x}^T\mathbf{y}$. To perform PPSP using lattice, there are four steps required. The following subsections describe each of them in details. The complete algorithm is given in Fig. 1.

4.0.1 System initialisation

Let us start with generating a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ which is known to X and Y. The matrix $\mathbf{A}$ contains column vectors $\mathbf{a}_1$, $\mathbf{a}_2$, ..., $\mathbf{a}_m \in \mathbb{Z}_q^n$ i.e., $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m]$.

4.0.2 Step 1

Entity X computes a SIS style vector using $\mathbf{A}$ and the binary vector $\mathbf{x}$ as

$$\mathbf{u} = \mathbf{Ax}\ (mod\ q) \in \mathbb{Z}_q^n, \tag{9}$$

and sends $\mathbf{u}$ to Y.

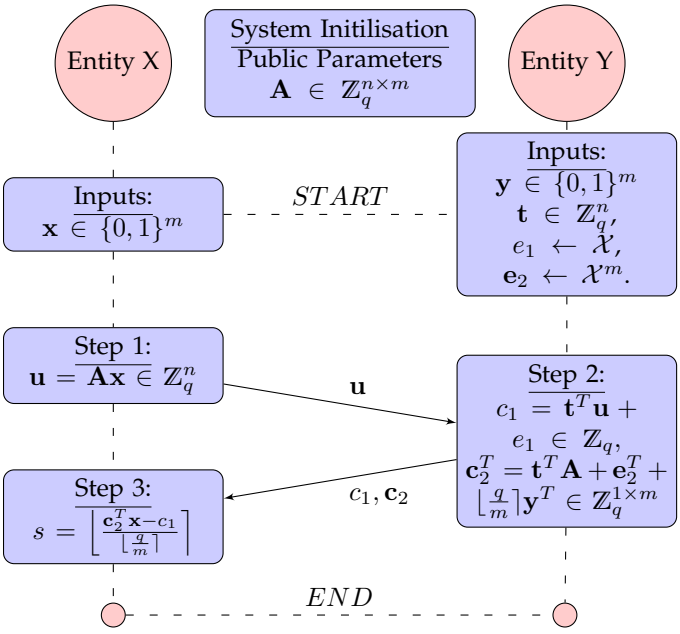

Fig. 1. Flow diagram for the proposed lattice-based privacy-preserving scalar product computation for binary vectors

4.0.3 Step 2

Entity Y generates a uniformly random vector $\mathbf{t} \in \mathbb{Z}_q^n$, a small error term $e_1 \leftarrow \mathcal{X}$, and a small error vector $\mathbf{e}_2 = [e_{2,1}, e_{2,2}, \ldots, e_{2,m}]^T \leftarrow \mathcal{X}^m$. Then Y computes the following LWE style term c_1 and vector $\mathbf{c}_2$:

$$c_1 = \mathbf{t}^T\mathbf{u} + e_1 \ (mod\ q) \in \mathbb{Z}_q, \quad (10)$$

$$\mathbf{c}_2^T = \mathbf{t}^T\mathbf{A} + \mathbf{e}_2^T + \lfloor\frac{q}{m}\rceil\mathbf{y}^T \ (mod\ q) \in \mathbb{Z}_q^{1\times m}, \quad (11)$$

and sends these to X.

4.0.4 Step 3

Entity X performs the following computation to retrieve the SP value $s = \mathbf{x}^T\mathbf{y}$ as follows:

$$s = \left\lfloor \frac{\mathbf{c}_2^T\mathbf{x} - c_1}{\lfloor\frac{q}{m}\rceil} \right\rceil. \quad (12)$$

4.1 Condition for Correctness

Let us derive the condition for the above-mentioned algorithm to output a correct result. In (12),

$$\begin{aligned}\mathbf{c}_2^T\mathbf{x} - c_1 &= (\mathbf{t}^T\mathbf{A} + \mathbf{e}_2^T + \lfloor\frac{q}{m}\rceil\mathbf{y}^T)\mathbf{x} - (\mathbf{t}^T\mathbf{u} + e_1),\\ &= \mathbf{t}^T\mathbf{Ax} + \mathbf{e}_2^T\mathbf{x} + \lfloor\frac{q}{m}\rceil\mathbf{y}^T\mathbf{x} - \mathbf{t}^T\mathbf{u} - e_1.\end{aligned}$$

Since $\mathbf{Ax} = \mathbf{u}$, and $\mathbf{t}^T\mathbf{Ax} = \mathbf{t}^T\mathbf{u}$,

$$\mathbf{c}_2^T\mathbf{x} - c_1 = \lfloor\frac{q}{m}\rceil\mathbf{y}^T\mathbf{x} + \mathbf{e}_2^T\mathbf{x} - e_1. \quad (13)$$

In (13), the scalar product is masked by error term $\mathbf{e}_2^T\mathbf{x} - e_1$. To output a correct answer, this error term must satisfy the following condition:

$$\mathbf{e}_2^T\mathbf{x} - e_1 < \lfloor\frac{q}{2m}\rceil, \quad (14)$$

hence,

$$\frac{\mathbf{e}_2^T\mathbf{x} - e_1}{\lfloor\frac{q}{m}\rceil} < \frac{1}{2}. \quad (15)$$

Therefore,

$$s = \left\lfloor \frac{\mathbf{c}_2^T\mathbf{x} - c_1}{\lfloor\frac{q}{m}\rceil} \right\rceil = \left\lfloor \frac{\lfloor\frac{q}{m}\rceil\mathbf{y}^T\mathbf{x} + \mathbf{e}_2^T\mathbf{x} - e_1}{\lfloor\frac{q}{m}\rceil} \right\rceil = \mathbf{y}^T\mathbf{x},$$

which proves the correctness of the proposed algorithm. Further, the requirements for the error term (14) should be analysed and defined such that $\mathbf{e}_2^T\mathbf{x} - e_1$ is always smaller than $\lfloor\frac{q}{2m}\rceil$. To achieve this, we need to find the upper bound for the error term. The following subsection is dedicated for this analysis.

4.2 Upper bound of the error term ($\mathbf{e}_2^T\mathbf{x} - e_1$)

As we described in Section 3.2.3, the small error terms are sampled from a normal distribution with mean 0 and standard deviation $\frac{\alpha}{\sqrt{2\pi}}$ (let us denote this as $\Psi_{0,\frac{\alpha}{\sqrt{2\pi}}}$) followed by scaling and modulo reduction by q as follows:

$$e = \lfloor wq \rceil (mod\ q) \quad (16)$$

where $w \leftarrow \Psi_{0,\frac{\alpha}{\sqrt{2\pi}}}$ and e belongs to a "rounded" normal distribution with mean 0 and standard deviation $\frac{\alpha q}{\sqrt{2\pi}}$ (let us denote this as $\mathcal{X}_{0,\frac{\alpha q}{\sqrt{2\pi}}}$).

Let us also denote vectors $\mathbf{w} = [w_1, w_2, \ldots, w_m] \leftarrow \Psi^m_{0,\frac{\alpha}{\sqrt{2\pi}}}$ and $\bar{\mathbf{w}} = [w_1, w_2, \ldots, w_{m+1}] \leftarrow \Psi^{m+1}_{0,\frac{\alpha}{\sqrt{2\pi}}}$. Hence the error vector

$$\mathbf{e} = \lfloor \mathbf{w}q \rceil (mod\ q). \quad (17)$$

Using the above information, let us find the upper bound for the error term $\mathbf{e}_2^T\mathbf{x} - e_1$. Let us define an $m+1$ dimensional vector $\bar{\mathbf{e}} = [\mathbf{e}_2^T\ e_1]^T$ and another $m+1$ dimensional vector $\bar{\mathbf{x}} = [\mathbf{x}^T\ -1]^T$, hence, $\mathbf{e}_2^T\mathbf{x} - e_1 = \bar{\mathbf{e}}^T\bar{\mathbf{x}}$. Using the triangle inequality, we can define the upper bound of the error term as follows:

$$|\mathbf{e}_2^T\mathbf{x} - e_1| = |\bar{\mathbf{e}}^T\bar{\mathbf{x}}| \leq |(\bar{\mathbf{e}} - q\bar{\mathbf{w}})^T\bar{\mathbf{x}}| + |(q\bar{\mathbf{w}})^T\bar{\mathbf{x}}|. \quad (18)$$

Using the Cauchy-Schwarz inequality [19], we can define the upper bound for the terms in (18) as follows:

$$|(\bar{\mathbf{e}} - q\bar{\mathbf{w}})^T\bar{\mathbf{x}}| < ||\bar{\mathbf{e}} - q\bar{\mathbf{w}}||.||\bar{\mathbf{x}}|| \quad (19)$$

$$|(q\bar{\mathbf{w}})^T\bar{\mathbf{x}}| < ||q\bar{\mathbf{w}}||.||\bar{\mathbf{x}}|| \quad (20)$$

According to (16) and (17), the rounding error for the components w is at most $\frac{1}{2}$ (i.e., $e - \lfloor wq \rceil \leq \frac{1}{2}$), we have $||\bar{\mathbf{e}} - q\bar{\mathbf{w}}|| \leq \frac{\sqrt{m+1}}{2}$ and $||\mathbf{e}_1 - q\mathbf{w}|| \leq \frac{\sqrt{m}}{2}$. Hence,

$$||\bar{\mathbf{e}} - q\bar{\mathbf{w}}||.||\bar{\mathbf{x}}|| + ||q\bar{\mathbf{w}}||.||\bar{\mathbf{x}}|| \leq \frac{\sqrt{m+1}}{2}||\bar{\mathbf{x}}|| + ||q\overline{\mathbf{w}}||.||\bar{\mathbf{x}}||.$$

Since $\bar{\mathbf{x}} \in \{0,1\}^{m+1}$, the Euclidean norm of $\bar{\mathbf{x}}$ is $||\bar{\mathbf{x}}|| \leq \sqrt{m+1}$. Hence,

$$\frac{\sqrt{m+1}}{2}||\bar{\mathbf{x}}|| + ||q\overline{\mathbf{w}}||.||\bar{\mathbf{x}}|| \leq \frac{m+1}{2} + ||q\overline{\mathbf{w}}||.\sqrt{m+1}.$$

Since $\overline{\mathbf{w}} \leftarrow \Psi^{m+1}_{0,\frac{\alpha}{\sqrt{2\pi}}}$ and $q\overline{\mathbf{w}} \leftarrow \mathcal{X}^{m+1}_{0,\frac{q\alpha}{\sqrt{2\pi}}}$, if we choose standard deviation as 4.5, then the probability

$$Pr\left(|qw| > 4.5 \times \frac{q\alpha}{\sqrt{2\pi}}\right) < 2.5 \times 10^{-7},$$

(i.e., one in four million). The probability will decrease further if we choose a higher number of standard deviations for the upper bound. Without loss of generality, in the rest of the paper, we consider standard deviation as 4.5. Therefore, with very high probability,

$$||q\bar{\mathbf{w}}|| \leq 4.5q\alpha\sqrt{\frac{m+1}{2\pi}}. \quad (21)$$

Therefore, with very high probability, the error

$$\begin{aligned} |\mathbf{e}_2^T\mathbf{x} - e_1| &\leq \frac{m+1}{2} + ||q\overline{\mathbf{w}}||.\sqrt{m+1}, \\ &\leq \frac{m+1}{2} + 4.5q\alpha\sqrt{\frac{m+1}{2\pi}}.\sqrt{m+1}. \end{aligned}$$

As long as this error is smaller than $\lfloor\frac{q}{2m}\rceil$, i.e.,

$$\frac{m+1}{2} + 4.5q\alpha\frac{(m+1)}{\sqrt{2\pi}} \leq \left\lfloor\frac{q}{2m}\right\rceil, \quad (22)$$

our proposed solution outputs a correct result. Hence, if the upper bound for α is

$$\alpha \leq \frac{\sqrt{2\pi}}{4.5q(m+1)}\left[\lfloor\frac{q}{2m}\rceil - \frac{m+1}{2}\right], \quad (23)$$

then with high probability (it may not provide correct result one in four million times), the proposed algorithm outputs a correct result. This concludes the proof for correctness. The requirements for the correctness are listed in Table 1.

Extending the inputs from {0,1} to integer inputs {0,1,2, . l} will lead to a smaller bin size i.e., $q/(m * l^2)$. Using this smaller size, the equations (14) to (23) can be revised to obtain parameters for input {0,1,2, . l}. The next section analyses the security of the proposed algorithm.

5 Security Analysis

As defined in Section 4 (refer to Fig. 1), the objective is to protect the privacy of $\mathbf{x}$ from Y and $\mathbf{y}$ from X. Entities X and Y interact with each other to compute the SP.

Firstly, let us prove that Y cannot learn the secret vector $\mathbf{x}$ from the exchanged vector $\mathbf{u}$ in Step 1. Since $\mathbf{x} \in \{0,1\}^m$ (therefore $\mathbf{x}$ is a short vector), according to the hardness of ISIS problem defined in Section 3.2, it is intractable for Y to solve $\mathbf{u} = \mathbf{A}\mathbf{x}\ mod\ q$ and obtain a short vector as a solution.

Step 1 operation is similar to hashing. Since the dimension of typical vector $\mathbf{x}$ is 10000, there are 2^{10000} possibilities. The only problem is (as same as in any hashing algorithm) the output of Step 1 is deterministic for same $\mathbf{x}$.

Therefore brute force approach may not work for Y. Hence Y needs to use mathematical properties to solve the problem to uncover $\mathbf{x}$ from $\mathbf{u}$. In other words, if Y can recover $\mathbf{x}$ from $\mathbf{u}$ then Y can solve the lattice hardest problem. As defined in Section 3.2, Y cannot find a vector $\mathbf{x}$ shorter than β i.e., $||\mathbf{x}|| < \beta$. Therefore, let us analyse the shortest possible vector which can be recovered by Y.

Suppose if Y wants to find a short vector $\mathbf{x}$ from $\mathbf{u} = \mathbf{A}\mathbf{x}\ mod\ q$ then Y may exploit the state-of-the-art techniques called lattice reduction method [14] and/or combinatorial method [15]. Denote the shortest vector which can be found by these techniques as $\mathbf{x}_s$. It is proven in literature (theoretically and experimentally) [17], that the Euclidean length of $\mathbf{x}_s$ has a lower-bound as follows:

$$||\mathbf{x}_s|| \geq min\left\{q, 2^{2\sqrt{n.log(q)log(\delta)}}\right\}, \quad (24)$$

where $\delta \geq 1.01$ [14]. Since the X's secret vector $\mathbf{x} \in \{0,1\}^m$, the Euclidean length $||\mathbf{x}|| \leq \sqrt{m}$. Hence, using (24) and assuming q is very large, if

$$\sqrt{m} < 2^{2\sqrt{n.log(q)log(\delta)}}, \quad (25)$$

then Y cannot recover $\mathbf{x}$ from $\mathbf{u}$. This is a first condition for security. This concludes that if condition (25) is met then Y cannot recover $\mathbf{x}$ from $\mathbf{u}$. Also, the cost (L) of finding a short binary vector using the techniques described above is defined as [17]:

$$L \approx 2^{\frac{m}{2^k}}, \quad (26)$$

where k should satisfy the following equation:

$$\frac{2^k}{k+1} \approx \frac{m}{n.log(q)}. \quad (27)$$

Now let us focus whether X can recover $\mathbf{y}$ from the messages c_1 and $\mathbf{c}_2$ sent by Y to X in Step 2.

According to the definition in Section 3.2, if c_1 and $\mathbf{c}_2$ are LWE terms then it is intractable for X to recover $\mathbf{y}$ since c_1 and $\mathbf{c}_2$ are indistinguishable from uniformly random distribution. If $\mathbf{t}$, $\mathbf{u}$, and $\mathbf{A}$ are uniformly distributed and the error term e_1 and error vector $\mathbf{e}_2$ are sampled from normal distribution with standard deviation greater than $2\sqrt{n}$ as defined in (8) then c_1 and $\mathbf{c}_2$ are uniformly random.

Matrix $\mathbf{A}$ is already a uniformly random matrix. Entity Y can generate uniformly random $\mathbf{t}$, e_1 and $\mathbf{e}_2$. The vector $\mathbf{u}$ sent by X is uniformly random as long as the number of possibilities for $\mathbf{x}$ is larger than $\mathbf{u}$ i.e., $2^m > q^n$ or $m > n.log(q)$ [17] (this is the second security condition).

Since the dimension of $\mathbf{t}$ is $m > 1$, and the scalar $\mathbf{t}^T\mathbf{u}$ is masked by an error term e_1, the term c_1 is scalar and completely random. Therefore, according to the LWE definition, it is intractable for X to recover the elements of $\mathbf{t}$ from scalar c_1. To analyse $\mathbf{c}_2$, let us denote the ith element of $\mathbf{c}_2$ as $c_{2,i}$ where $c_{2,i} = \mathbf{t}^T\mathbf{a}_i + e_{2,1} + \lfloor\frac{q}{2m}\rceil y_i$. In $c_{2,i}$, $\mathbf{t}^T\mathbf{a}_i + e_{2,1}$ is scalar and LWE term i.e., uniformly random. Similar to LWE encryption scheme [9], $\mathbf{t}^T\mathbf{a}_i + e_{2,1}$ acts like a one-time pad to hide the message $\lfloor\frac{q}{2m}\rceil y_i$. Hence, X cannot recover y_i from $c_{2,i}$ and therefore the proposed scheme is secure. In Section 5.1, we show that our parameter choice satisfying (8) (third security condition) is hard and at least equivalent to $128-$bit security.

In LWE, the noise term plays a major role in determining the hardness [9]. The normal distribution where the error terms are sampled must satisfy (8). The α term must be chosen as largest possible while satisfying (8) for hardness of LWE. To quantify the hardness or security level of LWE for a concrete set of parameters, Regev et. al exploited the dual lattice in [17, p. 21]. The idea is to find how many operations are required to distinguish an LWE term from uniform distribution. This is only possible if an adversary can find a short vector on dual lattice. To this, let us denote a vector $\mathbf{v}$ and denote a short vector in dual lattice as $\mathbf{w}$. If the vector $\mathbf{v}$ is an LWE vector then the scalar product $\mathbf{v}^T\mathbf{w}$ will be an integer [17, p. 22]. If not then $\mathbf{v}$ is a uniform random

TABLE 1
Requirements for Parameters to Achieve 128-bit security and Correctness when the standard deviation is set for 4.5.

	n	m
Correctness	$n \geq 1$	$m \geq 1$
Security	$n.log(q) > 128$	$m \geq nlog(q)$ & $\sqrt{m} < 2^{2\sqrt{nlog(q)log(\delta)}}$
	α	q
Correctness	$\alpha \leq \frac{\sqrt{2\pi}}{4.5q(m+1)} \left[\lfloor \frac{q}{2m} \rceil - \frac{m+1}{2}\right]$	$q > 2m$
Security	$\alpha \geq max\left\{\frac{2\sqrt{n}}{q}, 1.5\sqrt{2\pi}.max\left\{1/q, 2^{-2\sqrt{n.log(q).log(\delta)}}\right\}\right\}$	$q > n$

vector. Therefore finding a short vector in dual lattice must be hard. If the standard deviation of the error term $\alpha q/2\pi$ is not bigger than $1/||\mathbf{w}||$ then it may be possible to find a short vector in dual lattice. Therefore, error term must be bigger than $1/||\mathbf{w}||$ for LWE security. This requirement and (24) can now be used to quantify the LWE security.

Now using the lattice properties i.e., the length of a shorter vector in dual lattice is equivalent to $1/q$ times the length of shorter vector in lattice [17, p. 22]. Using this and (24), we can say $||\mathbf{w}|| \approx \frac{1}{q}.min\left\{q, 2^{2\sqrt{n.log(q)log(\delta)}}\right\}$. Therefore if error

$$\frac{\alpha q}{\sqrt{2\pi}} >> \frac{1}{||\mathbf{w}||}, \tag{28}$$

then LWE is hard. By taking 1.5 as factor, we can define the lower-bound for α from (28) as follows [17]:

$$\alpha \geq 1.5\sqrt{2\pi}.max\left\{1/q, 2^{-2\sqrt{n.log(q).log(\delta)}}\right\}. \tag{29}$$

The cost of finding a shorter vector is same as (26). In Section 5.1, we show that our parameter choice to satisfy (8) is hard and at least equivalent to $128-$bit security.

5.1 Parameter Selection

Firstly, let us obtain the relationship between q and m. Since the maximum possible value for $\mathbf{x}^T\mathbf{y}$ is m, we split q into m parts i.e., the distance between the consecutive values is $\lfloor \frac{q}{m} \rceil$. To obtain a correct result, as shown in (22), half of this distance should be larger to accommodate the error term i.e., $\lfloor \frac{q}{2m} \rceil > 1$ or $q > 2m$. Table 1 provides the necessary requirements for all the parameters to achieve correctness and security. This table is a summary of requirements derived in the previous sections. Using this table, let us obtain a concrete set of parameters to achieve $128-$bit security. The same strategy has been used to obtain the parameters for lower security (i.e., $80-$bits, and $112-$bits) and higher security $256-$bits in Section 6.

To obtain $128-$bit security, we need to choose our parameters in such a way that the cost equation (26), $L \approx 2^{\frac{m}{2^k}} \geq 2^{128}$. If we choose $k = 2$ then from (27), $m \approx n.log(q)$. Hence, $L \approx 2^{n.log(q)} \geq 2^{128}$. Therefore the security of the solution would be equal to $128-$bits if $n.log(q) \approx m \geq 128$. Based on this and other requirements (all are listed in Table 1), we are proposing six sets of parameters in Table 2 to achieve $128-$bits security. These parameters have been cross validated using the well known LWE Estimator [33] [- the source code for the LWE Estimator, that calculates the security complexity using six different algorithms such as lattice-reduction, dual-lattice attacks etc, is available at https://bitbucket.org/malb/lwe-estimator].

TABLE 2
Choices for the security parameters to achieve at least $128-$bit Security.

SET	n	m $\approx$	q $\approx$	$Security$ $\approx$	$\alpha.q$ (error std. $\approx$)
I	50	2^{15}	2^{570}	2^{128}	2^{538}
II	100	2^{15}	2^{270}	2^{128}	2^{238}
III	250	2^{15}	2^{116}	2^{128}	2^{85}
IV	500	2^{15}	2^{55}	2^{128}	2^{24}
V	1000	2^{15}	2^{39}	2^{187}	2^{7}
VI	2000	2^{16}	2^{41}	2^{517}	2^{7}

In Table 2, parameters n and q play a major role to ensure $128-$bit security. They are linked as increasing n leading to a small q. These parameters determine the size of matrix $\mathbf{A}$ and the memory requirement. The first four sets are equivalent in terms of memory ($\approx 100MB$) while the last two require around $200MB$ and $800MB$, respectively. As shown in the experiments, running time for the last two are significantly higher and not useful for practical applications. For Sets V and VI, the size of q is not decreasing as much as those for the other sets. The security levels for Sets V and VI are $187-$bits and $517-$bits, respectively. The reason is that, larger n leads to a larger m, hence, in order to satisfy the error distribution parameter α in (23), the value for q must be set to high. Increasing the value for α will increase the security.

6 Experimental Results

In order to evaluate the proposed LWE based PPSP scheme, we implemented the algorithm in Java and tested on a 64-bit Windows PC with 16GB RAM and Intel(R) Core(TM) i5-4210U CPU at 1.70GHz. For performance comparison, we also implemented the Paillier homomorphic encryption based PPSP scheme [21] on the same PC using Java. Additionally, we compared our scheme with one of the most efficient PPSP algorithms in [20]. Our test results show that the proposed LWE based scheme is significantly faster (at least 10^5 times faster) than the Paillier homomorphic PPSP scheme and at least twice as fast as [20] for the $128-$bit security.

TABLE 3
Paillier homomorphic encryption based PPSP [21].

Input by X: $\mathbf{a} = [a_1, \ldots, a_m]^T \in \{0,1\}^m$ and **Y:** $\mathbf{b} = [b_1, \ldots, b_m]^T \in \{0,1\}^m$
Output to X: $\mathbf{a}^T\mathbf{b}$
Step 1: X performs the following operations:
Generates Paillier public-private key pairs $\{pub, sk\}$,
FOR EACH a_i, $i = 1, 2, ..., m$
Computes
$E_{pub}(a_i) = [\![a_i]\!]$,
END FOR
keeps sk, and sends $(pub, E_{pub}(a_1) \ldots E_{pub}(a_m))$ to Y
Step 2: Y executes the following operations
Using b_i, $i = 1, 2, ..., m+2$
Computes
$E(\mathbf{a}^T\mathbf{b}) = [\![a_1]\!]^{b_1}.[\![a_2]\!]^{b_2} \ldots [\![a_m]\!]^{b_m}$
Sends $E(\mathbf{a}^T\mathbf{b})$ back to X
Step 3: X decrypts and obtains
$\mathbf{a}^T\mathbf{b} = D_{sk}(E(\mathbf{a}^T\mathbf{b}))$.

6.1 Proposed Lattice-based PPSP Scheme and Paillier PPSP scheme

The Paillier cryptosystem [21] is an additively homomorphic public-key encryption scheme. Its provable semantic security is based on the decisional composite residuosity problem: it is mathematically intractable to decide whether an integer z is an n-residue modulo n^2 for some composite n, i.e. whether there exists some $y \in \mathcal{Z}^*_{n^2}$ such that $z = y^n \mod n^2$. Let $n = pq$ where p and q are two large prime numbers. A message $m \in \mathcal{Z}_n$ can be encrypted using the Paillier cryptosystem as $[\![m]\!] = g^m r^n \mod n^2$ where $g \in \mathcal{Z}^*_{n^2}$ and $r \in \mathcal{Z}^*_n$. For a given encryption $[\![m_1]\!]$ and $[\![m_2]\!]$, an encryption $[\![m_1 + m_2]\!]$ can be obtained as $[\![m_1 + m_2]\!] = [\![m_1]\!][\![m_2]\!]$, and multiplication of an encryption $[\![m_1]\!]$ with a constant α can be computed efficiently as $[\![m_1.\alpha]\!] = [\![m_1]\!]^\alpha$. Hence, a Paillier cryptosystem is an additively homomorphic cryptosystem. Let us denote $E()$ and $D()$ as the Paillier homomorphic encryption and decryption functions. Using the homomorphic properties and the above definitions, homomorphic encryption based PPSP is described in Table 3.

According to NIST recommendation [31], [32], public-key encryption schemes such as RSA and Paillier must use $3072-$bit long keys for encryption and decryption in order to achieve $128-$bit security. Hence, to obtain the running time for the Paillier homomorphic encryption based PPSP, we used $3072-$bit long keys. We also obtained the running time for the proposed LWE based scheme for the first five sets of parameter given in Table 2 (Sixth set was ignored as it was taking too much time to run). The running times averaged over 100 executions are listed in Table 4 [no parallelization or multi-threading was used].

As presented in Table 4, the result of Set I has outperformed the other sets. This is due to the fact that, even though the security levels are equal across all the sets, when the size for n increases, the matrix $\mathbf{A}$ becomes larger and requires an increased number of multiplications. In turn, this slows down the algorithm. With this observation, we will continue using the parameters that belong to Set I for the remainder of our experiments presented in this paper.

TABLE 4
Average running time for the proposed and Paillier-based PPSP schemes.

SET	The Proposed Lattice-based PPSP				Pailler Based PPSP (ms)
	Step 1 (ms)	Step 2 (ms)	Step 3 (ms)	**Total (ms)**	
I	692	2482	21	3195	$\approx 5 \times 10^8$
II	756	3207	9	3972	$\approx 5 \times 10^8$
III	2456	7146	12	9614	$\approx 5 \times 10^8$
IV	4721	16972	9	21702	$\approx 5 \times 10^8$
V	129328	206741	8	336077	$\approx 8 \times 10^8$

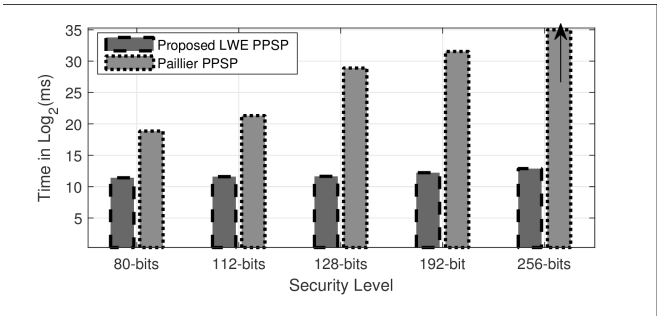

Fig. 2. Average running time for the proposed LWE PPSP scheme against the Paillier PPSP scheme for different security levels. Note that y-axis is in log scale.

The last column in Table 4 shows the average running time for the Paillier scheme. The proposed scheme is at least 10^5 times faster than Paillier PPSP scheme. The dimensions of the input vectors for these sets are in the range of 20000 to 50000 (see the third column in Table 2).

To compare the performance of the proposed scheme for different security levels, a new set of parameters are provided in Table 5. Based on the NIST recommendations [31], [32], the key sizes for the Paillier scheme is also provided in Table 5. Using this information, the average running time is plotted in Fig 2. While the average running time for the proposed scheme is increasing linearly, it increases exponentially for the Paillier scheme. It should be noted that the average running time for the proposed scheme is around 8 seconds at $256-$bit security [without any parallel computations or multi-threading]. These results demonstrate that the proposed lattice PPSP scheme is significantly faster than the Paillier PPSP.

TABLE 5
Parameters and key sizes for the proposed and Paillier based PPSP schemes for different levels of security.

Security	n	m $\approx$	q $\approx$	$\alpha.q$ $\approx$	Paillier Key Size
2^{80}	50	23500	2^{470}	2^{439}	1024
2^{112}	50	27500	2^{550}	2^{518}	2048
2^{128}	50	28500	2^{570}	2^{538}	3072
2^{192}	50	40500	2^{810}	2^{777}	7680
2^{256}	50	50000	2^{1000}	2^{997}	15360

6.2 Proposed Scheme and Randomisation Technique

Table 6 shows the state-of-the-art randomisation based PPSP [4], [20]. The security of this algorithm depends on the hardness of the factoring an integer i.e., $C_i = s(a_i.\alpha + c_i) \bmod p,\ a_i \neq 0$. C_is are protected by s and known only to X. If Y wants to recover the X's input vector, Y needs to factor all C_is to find the common s. This approach can be seen as an approach used in RSA encryption or any public-key encryption that relies on hardness of factoring integers. According to the NIST recommendation [31], [32], the size of these integers must be around $3072-$bit in order to obtain $128-$bit security (without loss of generality, we ignore the requirement of prime numbers). Hence, we set $k1$ in Table 6 to $3072-$bits to compare randomisation-based PPSP and the proposed lattice PPSP scheme.

Using this setting, the average running time for the proposed and randomisation based PPSP schemes are obtained at $128-$bit security. Fig. 3 shows the average running times for both schemes for different input vectors whose dimensions are between 30000 and 50000. The proposed scheme is at least twice as fast compared to randomisation based scheme for the security parameters. It should be noted that, since randomisation-based scheme relies on hardness of integer factorisation, similar to Paillier scheme, it is also vulnerable for quantum attacks.

TABLE 6
Randomisation based PP scalar product algorithm.

Input by X: $\mathbf{a} = [a_1, \ldots, a_m]^T \in \{0,1\}^m$ and **Y:** $\mathbf{b} = [b_1, \ldots, b_m]^T \in \{0,1\}^m$
Output to X: $\mathbf{a}^T\mathbf{b}$
Step 1: X performs the following operations:
Given security parameters k_1, k_2, k_3, k_4,
choose two large primes α, p
such that $\lvert p\rvert = k_1$, $\lvert\alpha\rvert = k_2$, set $a_{m+1} = a_{m+2} = 0$
Choose a large random number $s \in Z_p$, and $m+2$ random numbers c_i, $i = 1, 2, ..., m+2$, with $\lvert c_i\rvert = k_3$
FOR EACH a_i, $i = 1, 2, ..., m+2$
Compute
$C_i = s(a_i.\alpha + c_i) \bmod p,\ a_i \neq 0$
$C_i = sc_i \bmod p,\ a_i = 0$
END FOR
keeps $s^{-1} \bmod p$ secret, and sends $(\alpha, p, C_1 \ldots C_{m+2})$ to Y
Step 2: Y executes the following operations
set $b_{m+1} = b_{m+2} = 0$
FOR EACH b_i, $i = 1, 2, ..., m+2$
Compute
$D_i = b_i.\alpha.C_i \bmod p,\ b_i \neq 0$
$D_i = r_i.C_i \bmod p,\ b_i = 0$,
where r_i is a random number with $\lvert r_i\rvert = k_4$
END FOR
Send $D = \sum_{i=1}^{m+2} D_i \bmod p$ to X
Step 3: Now X computes and obtains
$E = s^{-1}.D \bmod p$ and get $\mathbf{a}^T\mathbf{b}$
$= \sum_{i=1}^{n} a_i.b_i = \frac{E-(E \bmod \alpha^2)}{\alpha^2}$.

Even though the proposed scheme is developed to protect the PP applications against the quantum computers, the efficiency analysis shows that the algorithm can be used to replace the existing schemes. Running time in Table 4 is obtained from sequential programming. It is taking around 3 seconds to execute the SP of two vectors whose dimensions are around 30000. Nearly 2.5 seconds are spent on Step 2 calculating (11). This equation can be computed in parallel i.e., $\mathbf{t}^T\mathbf{A}$ is equivalent to $\mathbf{t}^T\mathbf{a}_i$ where $i \leq m$. Therefore, we used multi threading features of Java to speed-up the process. By setting four threads, average running time has been reduced to 1.2 seconds from 3 seconds.

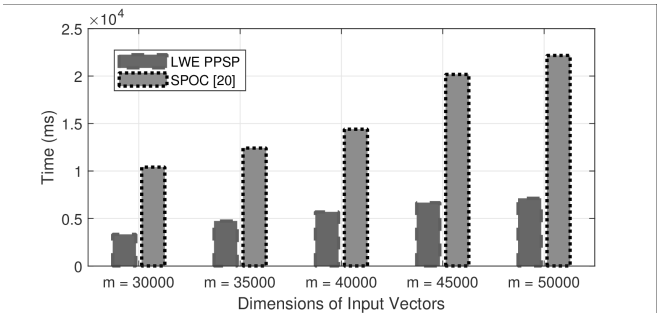

Fig. 3. Average running time for the proposed LWE PPSP scheme against the Randomisation-based PPSP scheme [4], [20] for different sizes of input vectors.

6.3 Communication Complexity

Using the algorithms in Fig. 1 (the proposed LWE scheme), Table 3 (Paillier Homomorphic Encryption Scheme based PPSP), and Table 6 (Randomisation based PPSP), we can calculate the communication cost in terms of transmitted bits between Entity **X** and Entity **Y**.

6.3.1 Total bits transmitted from Entity X to Entity Y

Total number of bits required to for the proposed LWE based PPSP scheme is $n * log_2(q)$. Similarly, $m * log_2(pub)$ and $(m+4) * log_2(k1)$ number of bits are required for the Paillier based scheme and Randomisation scheme, respectively.

6.3.2 Total bits transmitted from Entity Y to Entity X

Total number of bits required to for the proposed LWE based PPSP scheme is $(m+1) * log_2(q)$. Similarly, $log_2(pub)$ and $log_2(k1)$ number of bits are required for the Paillier based scheme and Randomisation scheme, respectively.

At 128-bit level security, if we extract the parameters, then $n = 50$, $log_2(q) = 570$, $log_2(pub) = 3072$, and $log_2(k1) = 3072$. Using these parameters, Table 7 shows the communication cost for all three schemes when the dimension of the input vectors is $m = 30000$. Its clear from Table 7 that the LWE scheme significantly benefits from a shorter prime number (six times smaller than the other schemes prime number) and achieves six times lower data requirement to perform the scalar computation.

TABLE 7
Communication cost comparison.

	X to Y	Y to X	Total
Proposed LWE PPSP	3.6 kB	2.1 MB	∼2 MB
Paillier PPSP	11.5 MB	0.3 kB	∼12 MB
Randomisation PPSP	11.5 MB	0.3 kB	∼12 MB

7 Conclusions and Future Work

In this paper a novel privacy-preserving scalar product computations using the fundamentals of lattice-based cryptography has been proposed. In particular, the proposed scheme was built directly on top of the lattice hard problems such as shortest integer solution and learning with errors. $128-$bit encryption security has been achieved with the proposed framework. Several validation and verification experiments have shown that the proposed scheme is one of the best performing scheme in terms of complexity whilst not compromising systems security.

Challenges and Future Work

The dimensions of the input vectors depend on n and q i.e., $m = n.log_2(q)$. Hence the proposed work supports larger dimensions such as 30000. Even though, this is appropriate for many applications, converting the solution to support smaller dimensions such as 100 would be an interesting problem that requires further investigations.

References

[1] Lagendijk, R. L., Erkin, Z., and Barni, M. (2013). Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. IEEE Signal Processing Magazine, 30(1), 82-105.

[2] Barni, M., Failla, P., Lazzeretti, R., Sadeghi, A. R., and Schneider, T. (2011). Privacy-preserving ECG classification with branching programs and neural networks. IEEE Transactions on Information Forensics and Security, 6(2), 452-468.

[3] Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., and Toft, T. (2009, August). Privacy-preserving face recognition. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 235-253). Springer, Berlin, Heidelberg.

[4] Rahulamathavan, Y., Sutharsini, K. R., Ray, I. G., Lu, R., and Rajarajan, M. (2019). Privacy-Preserving iVector-Based Speaker Verification. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 27(3), 496-506.

[5] Y. Rahulamathavan, R. Phan, S. Veluru, K. Cumanan, and M. Rajarajan, "Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud," *IEEE Trans. Dependable Secure Computing*, vol. 11, no. 5, pp. 467–479, Sept. 2014.

[6] Y. Rahulamathavan, S. Veluru, R. Phan, J. Chambers, and M. Rajarajan, "Privacy-preserving clinical decision support system using gaussian kernel based classification," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 1, pp. 56–66, Jan. 2014.

[7] Y. Rahulamathavan, R. Phan, J. Chambers, and D. Parish, "Facial expression recognition in the encrypted domain based on local fisher discriminant analysis," *IEEE Trans. Affective Computing*, vol. 4, no. 1, pp. 83–92, Jan.-Mar. 2012.

[8] Rahulamathavan, Y., Rajarajan, M. "Efficient Privacy-preserving Facial Expression Classification," *IEEE Trans. Dependable and Secure Computing* , in press.

[9] Regev, O., 2005. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In Proc. 37th ACM Symp. on Theory of computing (STOC), pages 84–93, 2005.

[10] Ajtai, M., 1996, July. Generating hard instances of lattice problems. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 99-108). ACM.

[11] Peikert, C., 2014, October. Lattice cryptography for the internet. In International Workshop on Post-Quantum Cryptography (pp. 197-219). Springer, Cham.

[12] Peikert, C., 2016. A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), pp.283-424.

[13] Regev, O., 2009. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), p.34.

[14] Gama, N. and Nguyen, P.Q., 2008, April. Predicting lattice reduction. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 31-51). Springer, Berlin, Heidelberg.

[15] Blum, A., Kalai, A. and Wasserman, H., 2003. Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM (JACM), 50(4), pp.506-519.

[16] Micciancio, D. and Peikert, C., 2012, April. Trapdoors for lattices: Simpler, tighter, faster, smaller. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 700-718). Springer, Berlin, Heidelberg.

[17] Micciancio, D., 2011. Lattice-based cryptography. In Encyclopedia of Cryptography and Security (pp. 713-715). Springer, Boston, MA. Available Online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.142.4862&rep=rep1&type=pdf [Last Accessed in December 2018]

[18] Agrawal, S., Freeman, D.M. and Vaikuntanathan, V., 2011, December. Functional encryption for inner product predicates from learning with errors. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 21-40). Springer, Berlin, Heidelberg.

[19] C. Meyer, *Matrix Analysis and Applied Linear Algebra*. In Society for Industrial and Applied Mathematics, ISBN 0-89871-454-0, 2000.

[20] R. Lu, H. Zhu, X. Liu, J. Liu, and J. Shao, Toward efficient and privacy-preserving computing in big data era, Network, IEEE, vol. 28, no. 4, pp. 4650, July 2014.

[21] P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, Proc. 17th Intl Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT 99), pp. 223-238, 1999

[22] Wang, Q., Hu, S., Ren, K., He, M., Du, M. and Wang, Z., 2015, September. Cloudbi: Practical privacy-preserving outsourcing of biometric identification in the cloud. In European Symposium on Research in Computer Security (pp. 186-205). Springer, Cham.

[23] Hu, S., Li, M., Wang, Q., Chow, S.S. and Du, M., 2018. Outsourced Biometric Identification With Privacy. IEEE Transactions on Information Forensics and Security, 13(10), pp.2448-2463.

[24] Du, W. and Atallah, M.J., 2001, December. Privacy-preserving cooperative statistical analysis. In Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual (pp. 102-110). IEEE.

[25] Du, W. and Zhan, Z., 2002, December. Building decision tree classifier on private data. In Proceedings of the IEEE international conference on Privacy, security and data mining-Volume 14 (pp. 1-8). Australian Computer Society, Inc..

[26] Vaidya, J. and Clifton, C., 2002, July. Privacy preserving association rule mining in vertically partitioned data. In Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 639-644). ACM.

[27] Amirbekyan, A. and Estivill-Castro, V., 2007, December. A new efficient privacy-preserving scalar product protocol. In Proceedings of the sixth Australasian conference on Data mining and analytics-Volume 70 (pp. 209-214). Australian Computer Society, Inc..

[28] Zhang, R., Zhang, Y., Sun, J. and Yan, G., 2012, March. Fine-grained private matching for proximity-based mobile social networking. In INFOCOM, 2012 Proceedings IEEE (pp. 1969-1977). IEEE.

[29] Dong, W., Dave, V., Qiu, L. and Zhang, Y., 2011, April. Secure friend discovery in mobile social networks. In INFOCOM, 2011 Proceedings IEEE (pp. 1647-1655). IEEE.

[30] Goethals, B., Laur, S., Lipmaa, H. and Mielikinen, T., 2004, December. On private scalar product computation for privacy-preserving data mining. In International Conference on Information Security and Cryptology (pp. 104-120). Springer, Berlin, Heidelberg.

[31] Elaine Barker; Allen Roginsky (November 6, 2015). "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST SP-800-131A Rev 1" (PDF). Nvlpubs.nist.gov. Retrieved 2016-09-24

[32] NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management" http://csrc.nist.gov/publications/PubsSPs.html800-57pt1r4

[33] Martin R. Albrecht, Rachel Player and Sam Scott. On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology. Volume 9, Issue 3, Pages 169203, ISSN (Online) 1862-2984, ISSN (Print) 1862-2976 DOI: 10.1515/jmc-2015-0016, October 2015

[34] Cheon, J.H., Kim, A. and Yhee, D., Multi-dimensional Packing for HEAAN for Approximate Matrix Arithmetics, Cryptology ePrint Archive, Report 2018/1245, 2018.

[35] Graepel, T., Lauter, K. and Naehrig, M., 2012, November. ML confidential: Machine learning on encrypted data. In International Conference on Information Security and Cryptology (pp. 1-21). Springer, Berlin, Heidelberg.

[36] Bos, J.W., Castryck, W., Iliashenko, I. and Vercauteren, F., 2017, May. Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling. In International Conference on Cryptology in Africa (pp. 184-201). Springer, Cham.
[37] Crawford, J.L., Gentry, C., Halevi, S., Platt, D. and Shoup, V., 2018, October. Doing real work with fhe: The case of logistic regression. In Proceedings of the 6th Workshop on Encrypted Computing and Applied Homomorphic Cryptography (pp. 1-12). ACM.

Yogachandran Rahulamathavan is a Senior Lecturer and Program Director for MSc Cyber Security and Big Data program at Loughborough Universitys London Campus in the UK. His research interest is on developing novel security protocols to advance machine learning techniques to solve complex privacy issues in emerging applications e.g., patients healthcare data sharing, biometric authentication systems, identity management in cloud, etc.

Currently, Dr Rahul is coordinating UK-India project (worth of 200k) between Loughborough University London, IIT Kharagpur and City, University of London. He is also an Associate Editor for IEEE Access Journal.

Safak Dogan is a Senior Lecturer in Multimedia Technologies at the Institute for Digital Technologies, Loughborough University London. His main areas of expertise include digital media signal processing, multimedia communication systems and networks, and quality assessment. His recent research focuses on data visualisation and user activity analysis for privacy protection. He has managed various EU-funded multinational collaborative research projects.

Xiyu Shi (M'15) received the B.Eng. degree in radio engineering from Southeast University, Nanjing, China, in 1984, the M.Sc. degree in communication and electronic systems from Beijing University of Aeronautics and Astronautics, Beijing, China, in 1989, and the Ph.D. degree in computer networks from Cranfield University, Shrivenham, UK, in 2002. From 2002 to 2004, he was with the Centre for Communication Systems Research (CCSR), University of Surrey, Guildford, UK. From 2004 to 2005, he was with the Department of Applied Computing, University of Buckingham, Buckingham, UK. In 2005, He re-joined the University of Surrey as a Research Fellow. He is currently a Lecturer at the Institute for Digital Technologies, Loughborough University London, UK. His research interests include IoT related privacy and security issues, cybersecurity, audio signal processing and multimedia communications.

Rongxing Lu (S'09-M'11-SM'15) is currently an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal", when he received his PhD degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific Outstanding Young Researcher Award, in 2013. He is presently a senior member of IEEE Communications Society. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise, and was the recipient of 8 best paper awards from some reputable journals and conferences. Currently, Dr. Lu currently serves as the Vice-Chair (Conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). Dr. Lu is the Winner of 2016-17 Excellence in Teaching Award, FCS, UNB.

Muttukrishnan Rajarajan received his BEng and PhD degrees from City University London in 1994 and 1999 respectively. From 1999 he worked at City University London as a Research Fellow. In August 2000 he moved to Logica as a Telecommunication Consultant. After a few years in the industry Raj is now a Professor of Security Engineering. He is also the Programme Director for the Engineering with Management and Entrepreneurship programme. He is a senior member of IEEE, a member of IET and an associate member of the institute of information security professionals (IISP) and a member of Technical Programme Committees for various prestigious conferences. He also sits on the Editorial boards of Springer/ACM Journal on Wireless Networks, Elsevier Journal of Health Policy and Technology and Emerald Journal of Information Management and Computer Security.

Ahmet Kondoz (M'91-SM'11) received the Ph.D. degree from the University of Surrey, U.K., in 1987, where he was a Research Fellow with the Communication Systems Research Group from 1986 to 1988 and became a Lecturer in 1988, a Reader in 1995, and in 1996 he was promoted to a Professor in multimedia communication systems. He was the Founding Head of I-LAB, a multi-disciplinary multimedia communication systems research lab with the University of Surrey. Since 2014, he has been the Founding Director of the Institute for Digital Technologies, Loughborough University London, a post graduate teaching, research, and enterprise institute.

His research interests include digital signal processing and coding, fixed and mobile multimedia communication systems, 3-D immersive media applications for the future Internet systems, smart systems such as autonomous vehicles and assistive technologies, big data analytics and visualization, and related cyber security systems. He has over 400 publications, including six books, several book chapters, and seven patents, and graduated over 75 Ph.D. students. He has been a Consultant for major wireless media industries and has been acting as an Advisor for various international governmental departments, research councils, and patent attorneys.

Dr. Kondoz has been involved with several European Commission FP6 FP7 research and development projects, such as NEWCOM, e-SENSE, SUIT, VISNET, and MUSCADE. Involving leading universities, research institutes, and industrial organizations across Europe. He coordinated FP6 VISNET II NoE, FP7 DIOMEDES STREP, and ROMEO IP projects, involving many leading organizations across Europe which deals with the hybrid delivery of high quality 3-D immersive media to remote collaborating users including those with mobile terminals. He co-chaired the European networked media advisory task force, and contributed to the Future Media and 3-D Internet activities to support the European Commission in the FP7 programmes.